Amendments to the Claims

Claims 1-8 (cancelled).

Claim 9 (previously amended): A method for preventing unauthorized alteration of content, comprising:

a) computing a hashed value for each executable command in a script;

b) encrypting the hashed value for each executable command in the script with a first public encryption private key, wherein the first public encryption private key uses a first private key to encrypt the hashed value for each executable command;

c) appending to the script the encrypted hashed values for each executable command;

d) providing a first public key corresponding to the first private key to a control program; and

e) signing the control program, comprising the script and the first public key, wherein signing the control program comprises encrypting the control program using a second public encryption private key, wherein the second public encryption private key uses a second public key, the signature for the control program for hiding the first public key provided therein.

Claims 10-12 (cancelled).

Claim 13 (previously amended): The method of claim 9, wherein the control program is an ActiveX control in an application program.

Claim 14 (original): The method of claim 13, wherein the ActiveX control is in a HyperText Markup Language (HTML) document.

Claim 15 (original): The method of claim 14, wherein the HTML document is downloaded from a HyperText Transfer Protocol (HTTP) server to a HTTP client.

Claim 16 (previously amended): A method for secure execution of content, comprising:

a) verifying a public key cryptography signature associated with a control program comprising a script;

b) computing a hashed value for each executable command in the script;

c) decrypting an encrypted hashed value appended to the script for each executable command in the script using a first public key to obtain a decrypted hashed value for each executable command in the script;

d) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

e) executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

Claim 17 (previously amended): The method of claim 16, wherein if the script is an encrypted script, further comprising decrypting the encrypted script with a symmetric encryption key to obtain the script.

Claim 18 (cancelled).

Claim 19 (previously amended): The method of claim 16, further comprising repeating b) and d) each execution of the executable commands in the script to prevent dynamic modification to the script.

Claim 20 (original): The method of claim 16, wherein the script is in a HyperText Markup Language (HTML) document.

Claim 21 (original): The method of claim 20, wherein the HTML document is downloaded to a Hypertext Transfer Protocol (HTTP) client from a HTTP server.

Claim 22 (original): The method of claim 21 performed by an ActiveX control in the HTML document.

Claim 23 (previously amended): An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) compute a hashed value for each executable command in a script;

b) encrypt the hashed value for each executable command in the script with a first public encryption private key, wherein the first public encryption private key uses a first private key to encrypt the hashed value for each executable command to the script;

c) append to the script the encrypted hashed values for each executable command;

d) provide a first public key corresponding to the first private key to a control program; and

e) sign the control program, comprising the script and the first public key, wherein instructions to sign the control program comprise instructions to encrypt the control program using a second public encryption private key, wherein the second public encryption private key uses a second public key, the signature for the control program for hiding the first public key provided therein.

Claim 24 (previously amended): An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) verify a public key cryptography signature associated with a control program comprising a script;

b) compute a hashed value for each executable command in the script;

c) decrypt an encrypted hashed value appended to the script for each executable command in the script using a first public key to obtain a decrypted hashed value for each executable command in the script;

d) compare the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

e) execute the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

Claim 25 (currently amended): An apparatus, comprising:

a server computer, the server computer including a database to house and serve web pages and a server processor to:

compute a hashed value for each executable command in a script on a web page;

encrypt the hashed value for each executable command in the script with a first public encryption private key, wherein the first public encryption private key utilizes a first private key to encrypt the hashed value for each executable command in the script;

append to the script the encrypted hashed values for each executable command;

provide a first public key corresponding to the first private key to a control program; and

sign the control program, comprising the script and the first public key, wherein to sign the control program includes to encrypt the control program using a second public encryption private key, wherein the second public encryption private key uses a second public key, the signature for the control program for hiding the first public key provided therein.

Claim 26 (previously amended): The apparatus of claim 25, further comprising:

a client computer having a client processor and a browser to enable a client to download the web page over a network, the client processor to:

compute a hashed value for each executable command in the script on the web page;

decrypt an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

compare the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

execute the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

Claim 27 (original): A method for creating secure content comprising:

a) hashing at least one executable command from a script in a web page to obtain a hashed value;

b) encrypting the hashed value using a private key A to generate a signed hashed value;

c) appending the signed hashed value to the script, wherein a public key A corresponding to the private key A is appended to the script; and

d) providing the public key A to a control within the web page, wherein the control is signed using a private key B to hide the public key A.

Claim 28 (original): The method of claim 27, wherein the script is enabled for execution upon activation of the signed control by a client receiving the web page.

Claim 29 (original): The method of claim 28, wherein activation of the signed control comprises the client clicking one of an applet and a button on the Web page.

Claim 30 (original): The method of claim 27, wherein the control comprises an ActiveX control.

Claim 31 (original): The method of claim 27, wherein prior to appending the signed hashed value to the script, encrypting the script, including the signed hashed value and the public key A, to provide a second level of encryption.

Claim 32 (original): The method of claim 31, wherein the second level of encryption comprises a symmetric key encryption.

Claim 33 (original): The method of claim 27, wherein a client downloading the web page activates the signed control, the method further comprising:

e) verifying the signed control using a public key B;

f) computing a hashed value for the at least one executable command in the script using an identical hashing function from a);

g) decrypting the at least one hashed executable command encrypted and appended to the script using public key A provided to the control;

h) comparing the computed hashed value for the at least one executable command in the script with the corresponding decrypted hashed value for the at least one executable command in the script; and

i) executing the executable commands in the script if the computed hashed values for the at least one executable command in the script are the same as the corresponding decrypted hashed values appended to the script for the at least one executable command.

Claim 34 (original): The method of claim 9, wherein appending to the script the encrypted hashed values for each executable command further comprises appending the first public key corresponding to the first private key used to encrypt the hashed value.

Claim 35 (currently amended): The method of claim 9, wherein computing a hashed value for each ~~executagle~~ executable command in the script comprises providing each executable command as a key value input to a hashing function, wherein the hashing function computes the hashed value corresponding to the executable.

Claim 36 (original): The method of claim 35, wherein the hashing function utilizes the first public key, which is tied to the script.

Claim 37 (original): The method of claim 9, further comprising encrypting the script, including the signed hashed values and the first public key, if present, with a symmetric key to provide another layer of encryption.

Claim 38 (original): The method of claim 16, wherein prior to verifying a public key cryptography signature associated with a control program, downloading a web page to enable a user to activate the control program, wherein the control program is contained in the web page.

Claim 39 (original): The method of claim 16, wherein verifying a public key cryptography signature associated with a control program comprising a script comprises:

decrypting the public key cryptography signature associated with the control program using a second public key, wherein the public key cryptography signature hides a first public key;

determining whether changes have occurred to either the control program or the public key cryptography signature associated with the control program; and

detecting the changes, if the changes have occurred.